Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claims 1-2 (Canceled).

3. (Currently Amended) The cryptography engine of claim [[1]] 68, wherein the cryptography engine is a DES engine.

Claim 4 (Canceled).

5. (Currently Amended) The cryptography engine of claim [[1]] 71, wherein the [[first]] second bit sequence is less than 32 bits.

6. (Currently Amended) The cryptography engine of claim [[1]] 71, wherein the [[first]] second bit sequence is four bits.

7. (Currently Amended) The cryptography engine of claim 5, wherein the ~~expanded~~ first bit sequence is less than 48 bits.

8. (Currently Amended) The cryptography engine of claim 6, wherein the ~~expanded~~ first bit sequence is less than six bits.

Claim 9-10 (Canceled).

11. (Currently Amended) The cryptography engine of claim [[9]] 68, wherein the ~~second~~ combined bit sequence is less than 32 bits.

12. (Currently Amended) The cryptography engine of claim [[10]] 68, wherein the ~~second~~ combined bit sequence is four bits.

13. (Currently Amended) The cryptography engine of claim [[1]] 68, ~~wherein the~~ further comprising a multiplexer circuitry including [[is]] a two-level multiplexer.

14. (Currently Amended) The cryptography engine of claim 13, wherein the two-level multiplexer is configured to select either initial data, swapped data, or non-swapped data to provide to [[the]] an output stage of the multiplexer.

15. (Currently Amended) The cryptography engine of claim [[1]] 68, wherein the inverse permutation ~~expansion~~ logic and the permutation logic are associated with DES operations.

16. (Currently Amended) The cryptography engine of claim [[1]] 68, wherein the key scheduler performs pipelined key scheduling logic.

17. (Currently Amended) The cryptography engine of claim [[1]] 68, wherein the key scheduler comprises a determination stage.

18. (Currently Amended) The cryptography engine of claim [[1]] 68, wherein the key schedule comprises a shift stage.

19. (Currently Amended) The cryptography engine of claim [[1]] 68, wherein the key scheduler comprises a propagation stage.

20. (Currently Amended) The cryptography engine of claim [[1]] 68, wherein the key scheduler comprises a consumption stage.

21. (Previously Presented) The cryptography engine of claim 17, wherein a first shift amount for a first key is identified in the determination stage using a first round counter value.

Claims 22 - 45 (Canceled).

46. (Currently Amended) The integrated circuit layout of claim [[44]] 73, wherein the cryptography engine in a DES engine.

Claim 47 (Canceled).

48. (Currently Amended) The integrated circuit layout of claim [[44]] 76, wherein the first bit sequence is four bits.

49. (Previously Presented) The integrated circuit layout of claim 48, wherein the expanded first bit sequence is less than six bits.

50. (Currently Amended) The integrated circuit layout of claim [[44]] 73, wherein the key scheduler performs pipelined key scheduling logic.

51. (Currently Amended) The integrated circuit layout of claim [[44]] 73, wherein the key scheduler comprises a determination stage, a shift stage, a propagation stage, and a consumption stage.

52. (Previously Presented) The integrated circuit layout of claim 51, wherein a first shift amount for a first key is identified in the determination stage using a first round counter value.

53. (Currently Amended) The integrated circuit layout of claim [[44]] 73, ~~wherein the~~ further comprising a multiplexer circuitry [[is]] including a two-level multiplexer.

54. (Currently Amended) The integrated circuit layout of claim 53, wherein the two-level multiplexer is configured to select either initial data, swapped data, or non-swapped data to provide to [[the]] an output stage of the multiplexer.

55. (Currently Amended) The integrated circuit layout of claim [[44]] 73, wherein the ~~expansion~~ inverse permutation logic and the permutation logic are associated with DES operations.

Claims 56 - 67 (Canceled).

68. (New) A cryptography engine for performing cryptographic operations on a data block having a first portion and a second portion, the cryptography engine comprising:

a key scheduler configured to provide keys for cryptographic operations;

means for combining via a first logical operation a particular key provided by the key scheduler with a first bit sequence associated with the first portion of the data block;

means for generating a second bit sequence based on the output of the first logical operation;

an inverse permutation logic performing an inverse permutation of a bit sequence associated with the second portion of the data block and generating an inverse permuted bit sequence;

means for combining via a second logical operation the second bit sequence with the inverse permuted bit sequence and generating a combined bit sequence; and

a permutation logic permuting the combined bit sequence and generating a permuted bit sequence.

69. (New) The cryptography engine of claim 68, wherein the first and second logical operations are binary XOR operations.

70. (New) The cryptography engine of claim 68, wherein the first bit sequence is a bit sequence expanded by an expansion logic.

71. (New) The cryptography engine of claim 70, wherein the second bit sequence is less than the first bit sequence.

72. (New) The cryptography engine of claim 68, wherein the data block contains bits 0 to M, the first portion contains bits 0 to N, and the second portion contains bits N+1 to M.

73. (New) An integrated circuit layout associated with a cryptography engine for performing cryptographic operations on a data block having a first portion and a second portion, the integrated circuit layout providing information for configuring the cryptography engine, the integrated circuit layout comprising:

a key scheduler configured to provide keys for cryptographic operations;

means for combining via a first logical operation a particular key provided by the key scheduler with a first bit sequence associated with the first portion of the data block;

means for generating a second bit sequence based on the output of the first logical operation;

an inverse permutation logic performing an inverse permutation of a bit sequence associated with the second portion of the data block and generating an inverse permuted bit sequence;

means for combining via a second logical operation the second bit sequence with the inverse permuted bit sequence and generating a combined bit sequence; and

a permutation logic permuting the combined bit sequence and generating a permuted bit sequence.

74. (New) The integrated circuit layout of claim 73, wherein the first and second logical operations are binary XOR operations.

75. (New) The integrated circuit layout of claim 73, wherein the first bit sequence is a bit sequence expanded by an expansion logic.

76. (New) The integrated circuit layout of claim 73, wherein the second bit sequence is less than the first bit sequence.

77. (New) The integrated circuit layout of claim 73, wherein the data block contains bits 0 to M, the first portion contains bits 0 to N, and the second portion contains bits N+1 to M.

78. (New) A cryptography engine for performing cryptographic operations on a data block, the cryptography engine comprising:

a key scheduler configured to provide keys for cryptographic operations;

an expansion logic expanding a bit sequence associated with the first portion of the data block and generating an expanded bit sequence having a first bit size;

a first XOR logic performing a first XOR operation of a first key provided by the key scheduler and the expanded bit sequence and generating a first combined bit sequence;

an Sbox logic taking the first combined bit sequence and generating a second bit sequence having a second bit size smaller than the first bit size;

an inverse permutation logic performing an inverse permutation of a bit sequence associated with the second portion of the data block and generating an inversed permuted bit sequence;

a second XOR logic performing a second XOR operation of the second bit sequence and the inverse permuted bit sequence and generating a second combined bit sequence; and

a permutation logic permuting the second combined bit sequence and generating a permuted bit sequence.

79. (New) The cryptography engine of claim 78, wherein the data block contains bits 0 to M, the first portion contains bits 0 to N, and the second portion contains bits N+1 to M.